DSS Secret Internet Protocol Router Network (SIPRnet) Processing Procedures

Introduction

DSS is the Cognizant Security Authority (CSA) for contractors participating in the National Industrial Security Program (NISP). The CSA's major role is oversight of industrial information systems. As CSA, DSS is the Designated Approving Authority (DAA) for industry classified information systems connecting to the Secret Internet Protocol Router Network (SIPRnet). DSS certifies and accredits classified industrial information systems in accordance with the NISPOM Ch 8.

DSS maintains continued oversight to ensure all required security controls are effectively implemented and sustained. Before any contractor-operated IS is authorized connection to the SIPRnet, they must be accredited by DSS to process classified information in accordance with reference (a), paragraph 8-200.   Additionally, DSS functions as the liaison between the contractor community and DISA.

Scope

The purpose of this section is to provide guidance for the implementation of SIPRnet connectivity to Industry.

Roles and Responsibilities

The following is a list of key participants and their responsibilities in the SIPRnet to Industry process.

Roles and Responsibilities

Participant(s)	Responsibilities
Defense Security Service	* Approval signatory on all System Security Plans (SSP) * Approval signatory on all Master SSPs.(MSSP) * Deciding official on revocation of accreditation and ISSM Certification Status with coordination with the RD, RDAA and DD FO.
Defense Information Systems Agency	* Connection Approval Authority * Responsible for circuit and oversight
Joint Staff	* Circuit validation with OSD approval
Government Sponsor	* Sponsor / Owner of Contractor Connection * Sponsor of Contractor Email and DNS * Provides funding for Circuit

DSS SIPRnet Program Management Office (PMO) disn@dss.mil	* Liaison between DISA and Industry * Customer Support

Government Sponsorship

The process to allow contractors to obtain SIPRnet connection begins with the Government Contracting Authority (GCA). A contractor must be sponsored by a GCA prior to obtaining access to SIPRnet. This sponsorship is required to validate contractor support and mission requirements.

The GCA sponsoring contractor SIRPNet connectivity must submit a sponsor request letter to Joint Staff requesting contractor access to SIPRnet. The sponsor request letter must include contract number, cage code, and point of contact information (i.e., name, address, telephone number, and e-mail). Additionally, the sponsor request letter should identify all SIPRnet resources the contractor will require access to (i.e., ports , protocols, services, websites, NATO requirements. etc.)

OSD Approval / J6 Validation

Joint Staff validates GCA sponsorship and forwards the sponsor request letter to OSD for approval. After OSD approves the SIPRnet request, Joint Staff forwards an approval letter to DISA and DSS.

As previously stated, the sponsor request letter should identify all SIPRnet resources requiring contractor access (i.e., ports and protocols, websites, NATO requirements and or etc.)

NOTE: *Contractors are not allowed unfiltered access to the SIPRnet. The Sponsor must complete a Disclosure Authorization (DA) form to identify contractor access requirements to the DISA SMC. The DISA SMC tracks and filters contractor access. The DA form can be obtained from and or forwarded to smc-ctr@disa.mil. Additionally, Joint Staff requires re-validation of contractor connections every 2 years. In the past Joint Staff validation letters were issued without expiration dates. Contractors should be advised to notify their Sponsor of the new validation requirement. The sponsor should submit a request for revalidation if their validation approval letter has exceeded a two year period.*

Questions regarding Joint Staff Validation should be directed to:

- CDR Joyce Bernard; COMM 703.697.4503 E-mail joyce.bernard@js.pentagon.mil

Or

- Lt Col Jodine K. Tooke; COMM 703.697.7611 E-mail jodine.tooke@js.pentagon.mil

DISA Control Number

Once DISA receives a copy of the approval letter from Joint Staff, a control number is assigned to the SIPRnet connection package. DISA then forwards (via e-mail) the Joint Staff approval letter and the associated control number to DSS Headquarters (HQ) and the sponsor. In addition, DISA will send an e-mail acknowledging receipt of the Joint Staff approval letter to the contractor.

DSS Notification to Field Representatives

After receiving formal approval by OSD, validation by Joint Staff and issuance of a control number by DISA, the DSS HQ SIPRnet Program Management Office (PMO) will forward a SIPRnet Security Information Package to the appropriate DSS Field Office Representative, who will work with the contractor to ensure proper completion of the security package. In addition, the DSS HQ SIPRnet PMO will also forward a Sponsor Information Package to the respective GCA.

The Security Information Package consists of:

- General Instruction Letter for IS Rep.
- General Instruction Letter for the contractor. This letter is designed to walk the contractor through Certification and Accreditation requirements as well as Connection Approval requirements. This letter will contain the signature of the IS Rep and will be forwarded to contractor by the IS Rep.
- SIPRNet Connection Question (SCQ). The SCQ is a DISA required document that must be completed in its entirety by contractor. The SCQ requires DAA signature. DAA Signature will be obtained at the time of accreditation decision/SSP approval. *NOTE: According to DISA, the SCQ is considered FOUO after completion and should not be sent to or from a contractor's commercial address.*
- Consent to Monitor Agreement template. This document must be completed and signed by the contractor.
- Residual Risk memorandum template. This document must be completed and signed by the contractor.
- SIPRnet Connection Questionaire (SCQ) *NOTE: According to DISA, the SCQ is considered FOUO after completion and should not be sent to or from a contractor's commercial address.*

The GCA Sponsor Package consists of:

- General Instruction Letter for the Sponsor.

- Disclosure Authorization (DA) Form. This form is used by the sponsor to request access to specific SIPRnet resources (i.e., Web Sites) on behalf of the contractor.

NOTE: *It is the DSS Field Representatives responsibility to work with the contractor to ensure the proper completion of the security package; however, it is the contractors' responsibility to forward the completed package DISA for a connection approval.*

Circuit Action

Once the control number is received and it is confirmed that the contractor is validated to host a SIPRnet connection, the sponsor should proceed with ordering the SIPRnet Circuit on behalf of the contractor. The circuit request should be directed to DDOE Customer Support 618-229-9922 (DSN-779) or the SIPRnet Support Center 1-800-582-2567. Additional information can be obtained via:
https://www.disadirect.disa.mil/products/asp/welcome.asp

DISA customer support will provide the sponsor with a packet containing information on how to contact the Joint Staff, as well as forms and procedures for getting the connection established.

Accreditation Process Outline for System with SIPRnet Connectivity

The information below outlines the accreditation process as it pertains to systems connecting to the SIPRnet.

- DSS HQ SIPRnet PMO forwards prepackaged notification memorandums and SIPRnet connection approval documents to the IS Rep in preparation for dissemination to the contractor

- IS Rep reviews/modifies prepackaged documents as necessary and forwards to Contractor.

- IS Rep/ISSP works with the contractor to prepare the system/site for accreditation. IS Rep/ISSP ensures the contractor is primed to submit the following required items:

    a) SSP + protection profile
    b) Network Topology Diagram
    c) Consent to Monitor memorandum completed with Contractor Signature
    d) SIPRnet Connection Questionnaire (SCQ) completed with site/system information. Form will eventually be signed by the DAA
    e) Statement of Residual Risk completed with Contractor signature
    f) Joint Staff validation letter

- DSS conducts a comprehensive review of the SSP and required connection approval documents.

- DSS approves the plan but rather than issue an IATO; notifies the Field Office Reps of system readiness for certification. IATOs are not issued to SIPRnet systems.

- Upon favorable verification/certification by DSS Field Operations DSS Field representatives will forward accreditation recommendation (Enclosure 28) to the DAA (RDAAor ODAA). **NOTE:** *In some cases the ISSP may submit an accreditation recommendation to the DAA in the absence of the encryptor and an installed circuit; however workstations and network infrastructure (Fireall and IDS) must be in place at the time of certification. However, if the contractor has at least met the Firewall requirement; a provisionary ATO may be issued to allow time for the contractor to implement an IDS solution. All new connections must implement an IDS and Firewall solution. The ISSP should verify contractor compliance with DISA network infrastructure requirements.*

- DAA rep reviews the package in its final state then forwards the security package to include the accreditation letter and SCQ to the DAA for signature. The ATO expiration date should coincide with date referenced in the Joint Staff letter.

NOTE: Systems with SIPRnet connectivity, requiring re-accreditation, should be reaccredited by DSS inspite of the absence of the Joint Staff approval letter. DSS should accredit the systems in increments of 3 years or to the term of the contract whichever expires first. At a minimum, DSS must take measures to validate the term of contract authorizing the contractor to process classified as well as ensure the sponsor is in the process of coordinating revalidation with Joint Staff.

SIPRnet Connection Approval

The DISA SIPRnet Connection Approval Office (SCAO) manages the Connection Approval Process (CAP) and security requirements for SIPRnet. Although DSS is the Designated Approval Authority (DAA) for classified contractor systems, DISA is the DAA for connection approval. DSS has no involvement with SIPRnet connection approval. The contractor is responsible for negotiating connection approval directly with DISA.

The contractor must submit the following documentation to the SCAO in support of connection approval:

System Security Plan (SSP)
Approval to Operate (ATO) memorandum
SCQ

Network topology diagram
Consent to Monitor Agreement memorandum
Residual Risk Statement memorandum
Joint Staff Validation letter

DISA will review the security documents and, if acceptable, will email an Interim Approval to Connect (IATC) to all associated POC's and schedule vulnerability testing. Once equipment is installed at the contractor site, DISA will conduct the vulnerability testing. The contractor must make arrangements to allow DISA through the firewall. Also, the firewall should only allow protocols authorized by DA process. When the contractor passes the vulnerability testing, DISA will email an Approval to Connect (ATC) to all associated POC's

Connection approval docs should be forwarded via e-mail to scao@disa.mil or mailed to:

DISA
P.O Box 4502
Arlington, VA. 22204-4502
Attn: GS211

Loop Away

DSS HQ SIPRnet Program Management Office (PMO) routinely compiles data for SIPRnet connection(s) that are set to expire between 30 and 180 days. The compiled data for the expiring connection(s) is organized in a spreadsheet with the SIPRnet circuits separated according to their expiration date in intervals of: 180-, 90-, 60-, 30- days and Expired. At the end of every month, the DSS SIPRnet PMO issues the spreadsheet (via e-mail) to DISA, the Field Office Chiefs (FOCs), Regional Directors (RDs) and Regional Designated Approval Authority (RDAAs) to review and provide updates as necessary. For the SIPRnet connection(s) that are expired and set to expire, e-mail messages are forwarded to the appropriate field representatives requesting status updates. At this time, the FOCs, RDs, RDAAs, IS Reps and ISSPs should provide DSS SIPRnet PMO with any status updates or re-accreditation/re-validation letters to prevent contractor connections from being looped away.

The PMO updates the Loop-Away List daily, with any status that is received, and updates DISA with the Loop-Away List bi-weekly. This serves as a way to compare and verify the status of the expired connections, between the two agencies. DISA updates their Global Information Grid (GIG) Interconnection Approval Process (GIAP) database with the information for the SIPRnet connections that the SIPRnet PMO provides. In addition, the Loop-away List will be provided monthly to the DSS CIO for input to the USD/I report to the Flag Panel.

If status (for example, a re-accreditation/re-validation letter) is not submitted by the end of the 30 day notice, the connection is no longer "valid" and will be recommended for looping-away. There will not be any grace period. However, if a unique situation warrants an extension, one may be granted, under the discretion of the DAA.

Input and questions regarding loop away status and processes should be forwarded to disn@dss.mil.

Contractor's Interaction with DISA

The contractor's sponsor is the main POC for requesting information from DISA. Any required action, not having to do with an Authority to Connect (ATC), is the responsibility of the sponsor.

Contractor interaction with DISA should be limited to security relevant inquiries (i.e., issues with IATC/ATC, expiring circuits.). These security relevant questions should be routed to scao@disa.mil or Mr. Zahid Sheikh (Office: 703.882.1940 Email:Zahid.Sheikh.ctr@disa.mil.) All other inquires (i.e., status of encryptor, circuit and or etc.) should be routed through the contractor's Government Sponsor to the identified Telecommunications Certification Office (TCO).

DISA Boundary Requirements

Joint Staff, in coordination with DISA, requires that all SIPRnet sites be configured with a Firewall and Intrusion Detection (IDS) System. Requirements for the Firewall/IDS selection and configuration are found in the DISA Security Technical Implementation Guide (STIG) for Network Infrastructure, Version 6, Release 4 at URL: http://iase.disa.mil/stigs/stig/network-stig-v6r4.pdf, and DISA STIG Enclave Security, Version 3, Release 1, dated 28 July 2005.

The Network Infrastructure STIG calls for a National Information Assurance Partnership (NIAP) evaluated and validated at EAL- 4 Firewall (EAL 4); and Intrusion Detection System (IDS) that is equivalent to the established US Protection Profile identified by the red PP on the NIAP webpage. For questions relating to approved boundary devices please contact the SIPRnet SCAO at 703-882-1455.

Note: *Special caveats such as CNWDI and Cryptovariable information may not be transmitted or received over the SIPRnet unless additionally encrypted with a Type 1 encryptor. Contractor Transmission of NATO across SIPRnet requires approval from Joint Staff.*